



**An Agency of
Industry Canada**

**Office de la Propriété
Intellectuelle
du Canada**

**Un organisme
d'Industrie Canada**

(11) **CA 2 300 343**

(13) **A1**

(40) 10.09.2000

(43) 10.09.2000

(12)

(21) 2 300 343

(51) Int. Cl.⁷:

H04L 012/66, H04L 009/32,
H04L 012/56

(22) 09.03.2000

(30) 9905509.7 GB 10.03.1999

(71)

NORTEL NETWORKS CORPORATION,
World Trade Center of Montreal
380 St. Antoine Street West
8th Floor, MONTREAL, Q1 (CA).

(72)

MAUGER, ROY (GB).

(74)

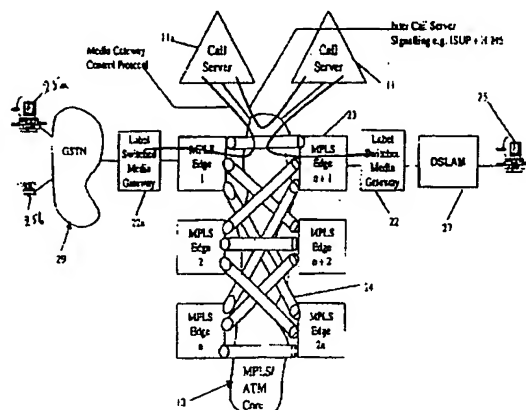
SMART & BIGGAR

(54) PASSERELLE DE SUPPORT COMMUTE PAR ETIQUETTE ET RESEAU

(54) LABEL SWITCHED MEDIA GATEWAY AND NETWORK

(57)

A network arrangement for delivering IP services to subscribers comprises a core network, a plurality of label switched media gateways coupled to the network and each providing an interface for one or more subscriber terminals. Call servers associated with the network are used to establish connections between pairs of gateways, these connections being routed across the core network via tunnels established therein. The tunnels are exclusively reserved for traffic between the label switched media gateways so as to provide security of that traffic from third party access and to provide a guaranteed quality of service. Because traffic is accepted into a tunnel only if bandwidth is available in that tunnel, firm and meaningful quality of service guarantees can be given to users.





(72) MAUGER, ROY, GB

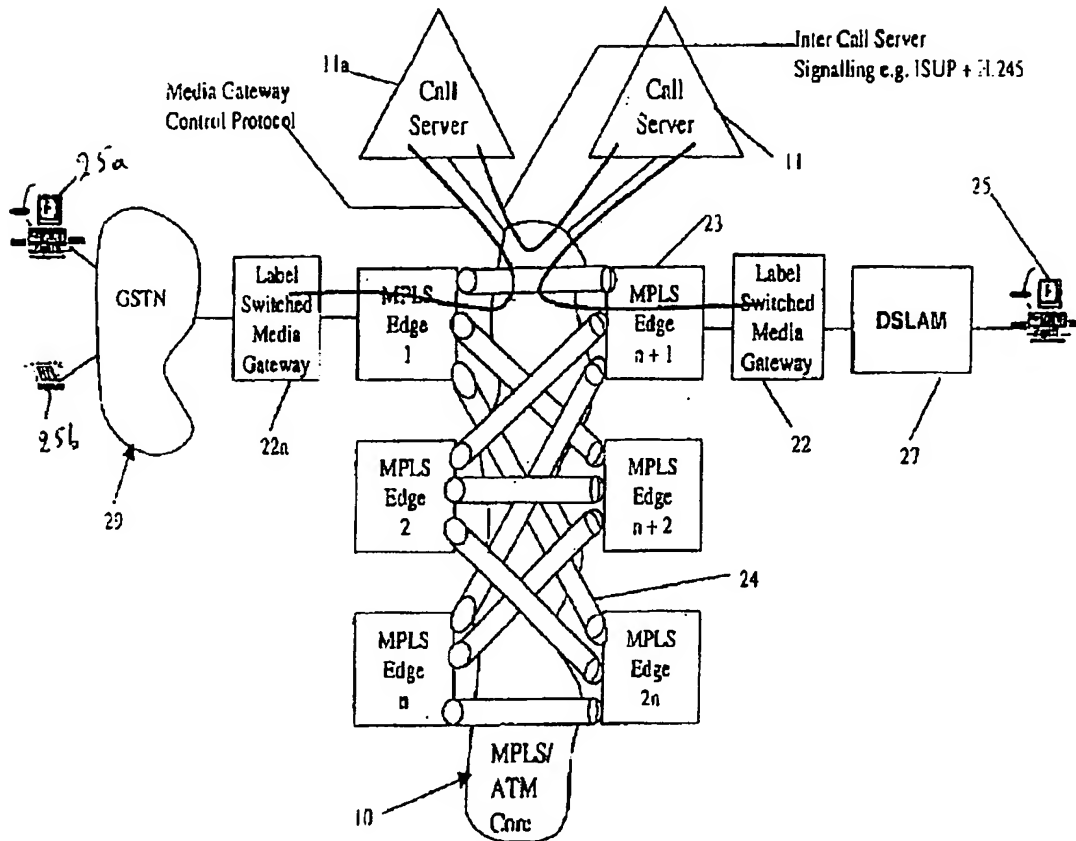
(71) NORTEL NETWORKS CORPORATION, CA

(51) Int.Cl.⁷ H04L 12/66, H04L 12/56, H04L 9/32

(30) 1999/03/10 (9905509.7) GB

(54) **PASSERELLE DE SUPPORT COMMUTE PAR ETIQUETTE ET
RESEAU**

(54) **LABEL SWITCHED MEDIA GATEWAY AND NETWORK**



(57) A network arrangement for delivering IP services to subscribers comprises a core network, a plurality of label switched media gateways coupled to the network and each providing an interface for one or more subscriber terminals. Call servers associated with the network are used to establish connections between pairs of gateways, these connections being routed across the core network via tunnels established therein. The tunnels are exclusively reserved for traffic between the label switched media gateways so as to provide security of that traffic from third party access and to provide a guaranteed quality of service. Because traffic is accepted into a tunnel only if bandwidth is available in that tunnel, firm and meaningful quality of service guarantees can be given to users.



5

ABSTRACT

LABEL SWITCHED MEDIA GATEWAY

10 A network arrangement for delivering IP services to subscribers comprises a
core network, a plurality of label switched media gateways coupled to the
network and each providing an interface for one or more subscriber terminals.
Call servers associated with the network are used to establish connections
between pairs of gateways, these connections being routed across the core
network via tunnels established therein. The tunnels are exclusively reserved
15 for traffic between the label switched media gateways so as to provide security
of that traffic from third party access and to provide a guaranteed quality of
service. Because traffic is accepted into a tunnel only if bandwidth is available
in that tunnel, firm and meaningful quality of service guarantees can be given to
users.

ID1121

LABEL SWITCHED MEDIA GATEWAY AND NETWORK

This invention relates to communications (IP) networks and in particular to the provision and delivery of services including data and voice services to subscribers over such networks.

5 BACKGROUND OF THE INVENTION

- Broadband networks are becoming widely used to deliver services such as video, data and voice services to customers. Typically, these services are transported in packets in a connectionless manner using e.g. the Internet protocol (IP). Routing of packets within such a network is determined from
- 10 information contained in the packet headers. These services originate from service providers, and a typical subscriber will have accounts with a number of these service providers. A particular problem in such an arrangement is that of providing each subscriber with the quality of service which he requires or demands for each particular service. This can be extremely difficult as the
- 15 priority bits that are placed in the packet headers and are used in one network to identify the quality of service that has been guaranteed can become meaningless when the traffic passes through several nodes. It will be appreciated that different services will have different quality of service requirements ranging from the high quality demands of real time services, such
- 20 as voice, to the best effort requirements of certain data services. In order to deliver such services, the network must be able to identify each service requirement and to provide sufficient bandwidth to deliver that requirement. This is not always possible with existing networks.
- 25 A further problem is that of maintaining security of a user's traffic from potential eavesdroppers in order to protect the content of the transmitted information. This can be a critical issue e.g. for financial institutions. Currently, this protection can only be effected by encryption, but this can be both complex and expensive to provide. Additionally, some forms of encryption may be subject to
- 30 legal restrictions where traffic is carried across national borders.

Reference is here directed to my co-pending applications serial No. 09/190,083; serial No. 09/190,082; and serial No. 09/190,081 which relate to methods and apparatus for label switching in connectionless e.g. IP networks.

5

SUMMARY OF THE INVENTION

An object of the invention is to minimise or to overcome the above disadvantages.

- 10 A further object of the invention is to provide an improved arrangement and method for delivery of network services to a subscriber.

- 15 According to a first aspect of the invention, there is provided a network arrangement for delivering IP packet services to subscribers, wherein said services are transported in tunnels established across the network whereby to provide security of that traffic from third party access and to provide a guaranteed quality of service to traffic accepted into a said tunnel.

- 20 According to another aspect of the invention, there is provided a method delivering IP packet services to network subscribers, the method comprising establishing tunnels in the network, transporting said services in the tunnels whereby to provide security of that traffic from third party access, and accepting traffic into a said tunnel only where capacity is available so as to provide a guaranteed quality of service to traffic accepted into that tunnel.

- 25 According to a further aspect of the invention, there is provided a label switched media gateway for controlling subscriber access to a connectionless core network in which user traffic is routed via tunnels established therein, the gateway providing an interface between a plurality of subscriber terminals and
30 being arranged to route user traffic across the network via tunnels of guaranteed capacity reserved for that traffic.

According to another aspect of the invention, there is provided a network arrangement for delivering IP services to subscribers, the arrangement

comprising a core network, a plurality of label switched media gateways coupled to the network and each providing an interface for one or more subscriber terminals, a plurality of call servers associated with the network and arranged to establish connections between pairs of said gateways, and
5 wherein said connections are routed across the core network via tunnels established therein, said tunnels being exclusively reserved for traffic between the label switched media gateways so as to provide security of that traffic from third party access and to provide a guaranteed quality of service.

10 According to a further aspect of the invention, there is provided a method of controlling subscriber access to a connectionless network so as to provided controlled delivery of services to that subscriber, the method comprising routing traffic to and from said subscribers via tunnels established across the network, and controlling admission to a said tunnel by determining the currently
15 available capacity of that tunnel so as to provide quality of service guarantees to accepted traffic.

According to a further aspect of the invention, there is provided a network arrangement for delivering IP services to subscribers, the arrangement
20 comprising a core network, a plurality of label switched media gateways coupled to the network via respective edge nodes and each providing an interface for one or more subscriber terminals, a plurality of tunnels arranged in the core network in a full mesh between said edge nodes, each said tunnel having a predetermined traffic handling capacity and each being exclusively
25 reserved for carrying traffic between a respective pair of said edge nodes, a plurality of call servers associated with the network and arranged to establish connections between pairs of said gateways via the respective edge nodes and tunnel, and wherein said call servers are arranged to determine the traffic occupancy of each said tunnel so as to accept new traffic into that tunnel only if
30 sufficient capacity is available in that tunnel so as to provide a guaranteed quality of service for accepted traffic.

According to another aspect of the invention, there is provided a method of controlling subscriber access via edge nodes to a connectionless network so

as to provided controlled delivery of services to the subscribers, the method comprising establishing a plurality of tunnels arranged in the network in a full mesh between said edge nodes, each said tunnel having a predetermined traffic handling capacity and each being exclusively reserved for carrying traffic
5 between a respective pair of said edge nodes, determining in response to each subscriber request for service the available capacity of a said tunnel in which the subscriber traffic is to be routed, and accepting that subscriber request for service only if sufficient capacity is available in that tunnel so as to provide quality of service guarantees to accepted traffic.

10

According to another aspect of the invention, there is provided a label switched media gateway for controlling subscriber access to a connectionless (IP) core network in which user traffic is routed via tunnels established therein, the gateway providing an interface between a plurality of subscriber terminals and
15 the network, and being arranged to route user traffic across the network via tunnels of guaranteed capacity reserved for that traffic, the gateway comprising a plurality of proxies for translating IP addresses between the network and encapsulated Layer 3 addresses, the latter constituting an address space which is allocated dynamically for session services to said subscribers.

20

The label switched media gateway (LSMG) is placed at the customer access point of an IP network in order to enhance the services offered by the IP network operator to the subscriber. In particular, the gateway construction allows the IP network operator:

25

- To offer the full range of PSTN/ISDN services as well as IP derived services.
- To offer quality of service for the services supplied to customers with the same guarantees as currently offered on PSTN/ISDN or ATM networks.
- To offer security from eavesdropping or malicious intrusion to customers
30 using the network without needing to resort to the expense and complexity of encryption.
- To allow the provision of extranet service between different users whilst maintaining security from eavesdropping and malicious intrusion from third parties without needing to resort to encryption.

5 In a preferred embodiment, traffic is routed across the network in dedicated tunnels which are reserved for the exclusive use of the label switched media gateways thus preserving security of the user traffic without the need for encryption. The call servers are aware of the current status of the network and the current occupancy of each tunnel bandwidth resources. Because traffic is accepted into a tunnel only if bandwidth is available in that tunnel, firm and meaningful quality of service guarantees can be given to users.

10 The tunnels may be provided on a permanent basis, or they may be established on demand.

15 In a preferred arrangement, routing of IP packets is performed by appending two labels to each IP packet, the first label identifying the tunnel to be used, and the second identifying the destination gateway for that packet.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described with reference to the accompanying drawings in which:-

20

Figure 1 shows a control environment for an IP network within which call servers are deployed on the IP network in order to offer switched services to customers;

25

Figure 2 illustrates a network arrangement according to a preferred embodiment of the invention;

30

Figure 3 illustrates a network arrangement according to another preferred embodiment of the invention which allows greater network scaling;

Figure 4 illustrates the method by which IP addresses are managed within the networks of figures 2 and 3;

Figure 5 illustrates the security mechanisms provided by the LSMG/MPLS networks of figures 2 and 3;

5 Figure 6 shows the functional architecture of a label switched media gateway (LSMG node) employed in the networks of figures 2 and 3;

Figure 7 shows the components of the traffic path or traffic module of the LSMG node of figure 6

10 Figure 8 illustrates the software components, deployed on servers, which are required to control the LSMG traffic path; and

15 Figure 9 shows by way of example a message sequence or flow chart for establishing a PSTN call using the LSMG/MPLS/call server architecture in the networks of figures 2 and 3;

DESCRIPTION OF PREFERRED EMBODIMENT

Referring first to figure 1, which is introduced for explanatory and comparative purposes, this shows in schematic form an exemplary control environment for an IP network 10 delivering services from one or more service providers to subscribers. The arrangement comprises two main components, a call server 11 and a media gateway 12, the latter providing an interface between the IP network 10 and a client terminal (not shown). The call server may for example be embedded in a H.323 gatekeeper 13 as shown, or it may be an independent entity. The call server 11 is intended to provide the full set of PSTN and ISDN services as well as IP multimedia services. The media gateway is thus the access point between a customer's network and the IP Network 10 of the carrier offering the services to the customer.

30 In the network of figure 1, a media gateway control protocol (MGCP) is employed which allows the call server 11 to control the media gateway 12. In its current definition, the MGCP comprises two parts, a signalling part to manage simple line or trunk signalling systems and a connection control part which is able to make connections in IP, ATM, frame relay or other networks.

A signalling system is employed between the call servers 11, which is preferably based on existing signalling systems such as ISUP (ISDN User Part). In its simplest form this signalling system is required to communicate
5 between the call servers: -

- The information content of existing ISUP messages.
- The IP addresses of the two endpoints.
- Bandwidth and coding schemes for voice and video services.

The above requirements can be achieved by embedding, for example, H.245
10 capability messages into ISUP messages as user-to-user information elements. This is assumed for the purpose of the following description, but it will of course be understood that the system will function with any signalling system, which achieves the same set of requirements.

15 The system is able to work with external terminals, which may comprise the following: -

- Simple lines and trunks controlled via MGCP signalling, which may be directly connected to a media gateway or remotely connected via an IP access network to a media gateway.
- 20 • Trunks connected directly or indirectly to a media gateway and controlled via SS7 signalling directly signalled to the call server.
- H.323 terminals connected to a media gateway over an IP access network.

A fully featured call server would allow interworking and service transparency between all of these terminal types.

25

Figure 2 illustrates an exemplary carrier IP network according to a preferred embodiment of the invention and utilising and augmenting the general control architecture of figure 1. The media gateways shown in figure 2 comprise the label switched media gateways 22 to be described in further detail below.
30 These gateways 22 are connected to MPLS (multi-protocol label switching) edge switches or nodes 23, which are in turn connected to the core IP network 10. It will be appreciated that each call server 11 can service a number of label switched media gateways 11. The core IP network 10 provides MPLS tunnels 24, with guaranteed traffic contracts, in a full mesh between the MPLS edge

nodes 23 which support the label switched media gateways 22. MPLS tunnels are also referred to as explicit routed label switched paths (ERLSP). These MPLS tunnels are reserved for the exclusive use of the LSMGs 22. User terminals 25 may be coupled to the LSMGs 22 via a digital subscriber line access multiplexer (DSLAM) 27. The core IP network may be built from any suitable technology which permits the establishment of MPLS tunnels with traffic contracts and guarantees that these tunnels are secure from third party access or intrusion. ATM and native mode MPLS over optics are preferred examples of possible IP core network technologies, but the technique is not of course restricted to these particular technologies.

A further label switched media gateway 22a may provide access to a general switched telephone network (GSTN) 29, e.g. a PSTN, so as to deliver voice services to the subscriber terminals 25a, 25b via the network 10. It will be understood that a terminal may comprise e.g. a basic voice terminal (25b) or a PC terminal (25, 25a) providing a wide range of functionality.

It will be appreciated that each tunnel 24 through the MPLS/ATM core network of figure 2 will pass a number of intermediate MPLS nodes within the core. For the sake of clarity, these intermediate nodes have been omitted from figure 2.

When a pair of call servers 11, 11a operating on LSMGs 22, 22a at different locations in the network have exchanged call signalling, IP address and bandwidth information and are ready to establish a connection, then they issue MGCP (media gateway control protocol) connection control commands to the two LSMGs 22, 22a. These connection control commands instruct IP streams to be opened from the sources and routed to the destinations. It is possible in MPLS to explicitly route the IP packets from a source for a destination over the particular tunnel which links the source and destination MPLS edge nodes. This is achieved by appending two labels to the IP packet, the first label identifying the tunnel to be used, and the second identifying the destination LSMG on the destination MPLS edge node. This explicit routing can be achieved in a number of ways: -

- LSMGs may be aware of LSMG IP addresses and can hold information relating LSMG nodes to tunnel labels.
- MGCP tunnelling modes can be extended so as to control explicit routing in MPLS tunnels as well as L2TP (Layer 2 Tunnelling Protocol) tunnels.

5

As the call servers 11, 11a are able to force traffic on to tunnels 24 with traffic contracts, then the servers are able to perform explicit bandwidth accounting as they receive bandwidth information from the inter-call server signalling system for each of the traffic streams that they manage.

10

When a request for a new call session or a new traffic stream is received, it is thus possible to reject or refuse the request if the corresponding tunnel bandwidth is currently exhausted with existing traffic. The tunnel bandwidth can be established based on traditional traffic engineering principles and the system dimensioned according to a grade of service and a guaranteed quality of service. If a call is accepted, then it is guaranteed a high quality of service. If this quality of service can not be guaranteed, then the call is rejected. The probability of a call being rejected is a function of the grade of service which is a design parameter relating the traffic predictions to the deployed bandwidth in the tunnels.

20

Telephony systems occasionally experience mass calling events in which the rate of call attempts can reach ten times that used for the dimensioning of the system resources. It is necessary in such circumstances to maintain the level of successful call completions in this environment, as this serves to drain away the excess demand. Experience has shown that if the rate of successful call completions is not maintained then the network can remain in a state of collapse for many hours, as users continue to repeatedly attempt calls which fail. Within an LSMG/MPLS network the call server is able to reject calls without needing to deploy any network resources to those failed calls. This mode of operation allows the rate of successful call completions to be sustained and allows mass calling events to be controlled by leaking away the excess demand.

25

30

Figure 3 illustrates an alternative embodiment incorporating a network architecture within which the explicit routing between edge nodes is forced over two tunnels in succession, e.g. 24a, 24b, with an intermediate MPLS node 31 which links the two tunnel endpoints. Within MPLS there are two possible ways of controlling explicit routing: -

- 5 • The originating LSMG can provide a stack of three labels identifying respectively the two tunnels and the destination LSMG. The first label is consumed on entry to the first tunnel, is translated at each intermediate MPLS node (not shown) along the tunnel 24a and is deleted at the
10 penultimate intermediate node (not shown) in order to expose the second tunnel label at the intermediate node 29. This process is then repeated to expose the label for the destination LSMG at the destination MPLS node.
- 15 • The originating LSMG can have a label for each destination LSMG. The first MPLS node is configured to route this traffic over the first tunnel so it adds a second label for that tunnel. This second label is removed prior to
20 reaching the intermediate node providing the intersection between the two tunnels. This intermediate node is also configured to route the traffic over the second tunnel and adds a further label. By a repeat process the packet with the destination LSMG label reaches the correct destination MPLS node and is then routed to the LSMG.

Figure 4 illustrates an exemplary scheme for IP address allocation within the LSMG networks of figure 2 and 3. The LSMGs 22 have internal endpoints to the MGCP control protocol, which endpoints have respective IP addresses.
25 Clients using PPP (point to point protocol) access links normally work with dynamic IP addresses. When connected to an LSMG, the LSMG addresses are assigned to the PPP terminals. When an LSMG 22 is connected to a campus network 41, typically through a L2TP tunnel 24, then the campus network will assign IP addresses to users of each PPP session multiplexed
30 onto the L2TP tunnel.

When a service is provided from a campus network through a LSMG network to a PPP connected user then: -

- The user is known to the Internet via the IP address assigned by the campus network so that any packets sent to the user are routed to the firewall of the campus network.
- The assigned address is translated at the LSMG providing campus access into a LSMG IP address.
- The LSMG providing access to the PPP connected client provides the client with one of its IP addresses.
- Switched IP connections are made using MGCP to connect the IP addresses of the two LSMG internal addresses which are also end to end connections as a result of the access associations.

Small/Medium businesses 43 may act as host nodes or utilise LSMG IP addresses. Host nodes, e.g. associated with the campus network, use their own IP Addresses on access links. The LSMG provides IP address translation.

Figure 5 illustrates a number of security measures which are built into an LSMG. For virtual private Intranet (VPI) operation a tunnel is established between the VPI and the LSMG. Routing at Layer 3 uses VPI addresses to access the tunnel. It is assumed that the VPI implementation is based on Layer 2 segregation. The LSMG provides an extranet application proxy function. For RTP (Real Time Protocol) streams this is based on IP/UDP/RTP header compression within the session context. This implies RTP mux or L2TP between LSMGs. Call servers and LSMGs do not advertise themselves with their IP addresses, so that Layer 3 label switched routers have no means of acquiring routes to these entities. This restriction may be achieved in a number of ways: -

- LSMGs can be connected in a full mesh to all other LSMGs in MPLS tunnels, which are nested within the MPLS tunnels, which link the edge MPLS switches. This means that LSMGs only need to exchange information related to ERLSPs, not that related to general routing. As mentioned above, LSMG addresses are not advertised for Layer 3 routing. MGCP messages are interpreted as tunnel labels for explicit routing. Call servers are similarly secured.

- The LSMGs may use labels, which are pre-assigned by a management system and delivered directly to all LSMGs. The MPLS edge nodes can then use policy control to ensure that label exchange is prevented from leaving its domain.

5

MPLS nodes, LSMGs and call servers all use IP sec authentication on all control and signalling interfaces to ensure that unauthorised or malicious users are not able to use these nodes as a point of intrusion.

- 10 When Interworking a LSMG with a virtual private Intranet (VPI), a MPLS tunnel can be configured to the nearest VPI access point, and VPI address space is allocated to the LSMG users. Routing in the Intranet is effected through the appropriate tunnel accessed from its VPI end. It is assumed that the VPI uses a form of Layer 2 segregation between VPI instances, such as virtual router
- 15 sub-nets segregated by ATM VCs, such that no two VPIs share the same ATM VC.

- The LSMG performs an application proxy firewall function in behalf of the end user networks. That is the LSMG checks that the user behaviour is valid within
- 20 the context of the session as established. As an example, it would be theoretically possible for a user to negotiate the opening of a voice logical channel but to instead maliciously open a data channel. The use of IP/UDP/RTP header compression on an end to end PPP session would corrupt any such malicious data channel thus effectively preventing any such
- 25 unauthorised use.

- Figure 6 illustrates the logical architecture of the label switched media gateway (LSMG). Each individual customer is provided via the gateway with his own private Layer 3 routing environment. Routing is possible between user ports,
- 30 network ports, call server ports and virtual private network ports. Each port is provided with a proxy server function, which acts as a relay point for user packets. Each Layer 3 environment is fully encapsulated and communication between users is only possible via external ports using the security mechanisms described above. The proxy functions translate between internal

and external IP addresses. Each proxy provides a function related to the endpoint with which it is associated thus: -

- a customer proxy 61 controls the PPP session involved with the end user
 - a service proxy 62 manages the association of an end user with a server.
5 For instance a registration admission and status (RAS) of H.323 requesting a gatekeeper would be received and forwarded to a number of available. The service proxy is responsible in selecting from the respondents and providing a cut-through connection to the end user.
 - a network proxy 63 provides the endpoint with RTP multiplexing or L2TP
10 tunnelling functions.
 - a routing proxy 64 provides network address translations and other functions associated with access to a public or private or virtual private IP network.
- 15 An LSMG physical realisation comprises two parts, a traffic module figure 7) and a server (figure 8), the latter providing services for a group of traffic modules. It will be appreciated that a shared server may be co-located with a group of LSMGs, or it may be distributed over the network.
- 20 The realisation of the proxy functions is divided into two parts. The encapsulated Layer 3 is realised by a system of IP cut-through functions which explicitly record source and destination IP address and port numbers. If a packet is received for an established cut-through, that packet is forwarded
25 directly by the traffic module HW at wire speed. Packets without a cut-through are forwarded to the LSMG SW for analysis to identify the associated proxy function. This then culminates in a cut-through to allow forwarding of the session media components.
- 30 Proxies translate IP addresses between external network and encapsulated Layer 3. EL3 addresses are part of the LSMG address space which is dynamically allocated for session services.

Figure 7 shows an exemplary realisation of a traffic module of the LSMG of figure 6 assuming operation in an IP over ATM environment. The traffic path

- for established IP Connections and established PPP sessions is handled by the traffic module independently of the centralised LSMG server. The traffic module comprises three sub-modules, namely a processor 71 for embedded software, an ATM module 72 for external connectivity and an LSMG specific module 73 which provides hardware assistance to enable the traffic module to operate at wire speed. The traffic module operates on an IP cut-through basis. Where client server relationships have been established then these are cut through. This is achieved by storing source and destination IP addresses and port numbers in a content addressable memory (CAM). When an IP packet arrives, the content addressable memory is addressed with its source and destination IP addresses. If these addresses are present in the memory, then the traffic module is able to extract the corresponding IP address translation; IP/PPP/L2TP formatting and MPLS label information so that packet forwarding is fully contained within the hardware of the traffic module. The LSMG hardware is thus a highly featured IP packet processor able to process IP address translations, IP/PPP/L2TP over ATM formatting and MPLS labels, as well as providing a content addressable memory for recording IP cut-through address pairs.
- 20 The traffic path for established IP Connections and established PPP Sessions is handled by the traffic module independently of a centralised INAS Server

Figure 8 shows the corresponding logical architecture of the LSMG server. This comprises: -

- 25 • Software 801 for configuring PPP sessions and L2TP tunnels.
- Software 802 for progressing sessions to the point where a cut-through can be established in the traffic modules.
- Software 803 for controlling internal facilities of the traffic module such as:-
 - 30 • Tunnel switching between L2TP tunnels to enable end to end PPP sessions controlled via RADIUS or Diameter servers.
 - RTP multiplexing which may be used for efficient communication between media gateways.
 - Label management to enforce the explicit routing mechanism.
- An OS and comms platform 804.

Considering by way of example the operation of the system for H.323 client terminals: -

- 5 • When the PPP session is created between the user terminal and the LSMG then a connection is made with a LSMG IP address either by propagating it as a dynamic address to the terminal or by providing a translation between the supplied address and an arbitrary LSMG internal one.
- 10 • When the H.323 client application powers up it sends a broadcast Registration Admission and Status (RAS) message searching for a gatekeeper. The LSMG traffic module has no cut-through for this packet so it forwards the packet to its server. The server recognises that this is a RAS message, so it repeats the message as a multicast to the gatekeeper servers. One or more gatekeepers respond to the broadcast message with an IP address port identity back to the LSMG server. The LSMG server
15 selects one of the gatekeepers' bids and sets up a cut-through in the LSMG traffic module.
- 20 • The client terminal sends a RAS message to its gatekeeper requesting permission to make a call. Permission is returned including an IP address port for call signalling. The client terminal then sends a call signalling message to its gatekeeper, but the IP address for call signalling may be different from that for RAS messages. If so, the call signalling message is trapped and sent to the LSMG server. The LSMG server recognises that this is H.323 call signalling so as to enable the cut-through and forward the
25 message.
- 30 • Assuming that the H.245 messages are embedded in the call signalling messages for fast call set-up, then the gatekeeper/call server will receive enough information to determine that through connection is required. Connection between the two terminals is then established by:-
 - Establishing a cut-through in the LSMG traffic modules at either end.
 - Providing IP/PPP/L2TP formatting information.
 - Providing MPLS labels for the routing of packets end to end.

This is achieved by a combination of MGCP control commands (Create Connection, Modify Connection) and policy information supplied to the LSMG by its management system to enable it to correctly interpret the MGCP commands. Turning on of the voice or other media streams is independent of these operations and is achieved e.g. by H.245 open logical connection commands, which are sent by the gatekeeper to the client terminal. The LSMG operations guarantee that the voice packets will flow end to end with full quality of service (QoS) guarantees.

10

Figure 9 illustrates the operation of the system for a simple PSTN call, e.g. to provide voice over IP services. Normal telephone sets 81 are connected via respective multiplexers 82a, 82b and an IP access system to an LSMG 83a, 83b at either end of a carrier IP network. The diagram of figure 9 shows a message sequence to establish a successful call set-up between the two terminals (note that although MGCP messages are all acknowledged, these acknowledgements are not shown in figure 9 for clarity): -

1. When the calling line goes off hook, the associated telephone mux system 82a sends a MGCP Notify (NTFY) with endpoint and offhook parameters. The telephony mux 82a autonomously provides dial tone to the calling party and removes that dial tone on receipt of the first digit received from the calling party.
2. The call server 11a responds with a MGCP NotificationRequest message (RQNT) with a digit map to define the method for collecting digits.
3. The telephone mux 82a sends in the dialled number. NTFY (dialled No). At this point the telephony mux opens send and receive ports for voice traffic.
4. The call server 11a identifies the far end call server 11b from the dialled number and sends an Initial Address Message (IAM). This message contains e.g. a H.245 message defining G711 coding at 64 kb/s and the source LSMG IP address.
5. The far end call server 11b sends a RQNT (NotificationRequest message) with endpoint and ring parameters.

6. The far end call server 11b returns an Address Complete Message to the near end call server 11a with G711 coding, 84kb/s and the destination LSMG IP address.
- 5 7. The far end call server 11b sends a MGCP CreateConnection command (CRCX) to the far end telephone mux 82b opening Send and Receive paths and requesting ring tone to be returned.
8. The far end call server 11b sends a CRCX command to its LSMG opening send and receive paths.
9. The near end call server 11a sends a CRCX message to its LSMG 22a opening a receive path only. The call originator can now hear ring tone.
- 10 10. At some point the called telephone 81b is answered and a NTFY message is sent to the far end call server 11b.
11. The far end call server 11b returns an Answer message (ANM) to the near end call server 11a.
- 15 12. The near end call server 11a sends a MGCP ModifyConnection command to its LSMG 22a to set into send/receive mode. The call is now in the conversation phase.

20 When the call has been completed, then a release message can be transmitted from either end. This release message is forwarded as an MGCP Notify message to the corresponding call server 11a (11b) which call server then sends an ISUP Release message to the call server 11b (11a) at the far end. The connections are released using MGCP Release connection commands and the call is terminated in the normal manner with the exception that MGCP
25 messages are used to communicate with the LSMG rather than proprietary messages to the system's embedded peripherals.

30 It will be appreciated that, although particular reference has been made in the above description by way of example to use of the H.323 and H.245 protocols, the techniques described herein are in no way limited to use with these particular protocols but are of more general application.

It will be understood that the above description of a preferred embodiment is given by way of example only and that various modifications may be made by

those skilled in the art without departing from the spirit and scope of the invention.

CLAIMS:-

1. A network arrangement for delivering Internet Protocol (IP) packet services
5 to subscribers, wherein said packet services are transported in tunnels
established across the network whereby to provide security of that traffic
from third party access and to provide a guaranteed quality of service.
2. A network arrangement for delivering IP services to subscribers, the
10 arrangement comprising a core network, a plurality of label switched media
gateways coupled to the network and each providing an interface for one or
more subscriber terminals, a plurality of call servers associated with the
network and arranged to establish connections between pairs of said
15 gateways, and wherein said connections are routed across the core
network via tunnels established therein, said tunnels being exclusively
reserved for traffic between the label switched media gateways so as to
provide security of that traffic from third party access and to provide a
guaranteed quality of service.
- 20 3. A network arrangement for delivering IP services to subscribers, the
arrangement comprising a core network, a plurality of label switched media
gateways coupled to the network via respective edge nodes and each
providing an interface for one or more subscriber terminals, a plurality of
25 tunnels arranged in the core network in a full mesh between said edge
nodes, each said tunnel having a predetermined traffic handling capacity
and each being exclusively reserved for carrying traffic between a
respective pair of said edge nodes, a plurality of call servers associated
with the network and arranged to establish connections between pairs of
30 said gateways via the respective edge nodes and tunnel, and wherein said
call servers are arranged to determine the traffic occupancy of each said
tunnel so as to accept new traffic into that tunnel only if sufficient capacity is
available in that tunnel so as to provide a guaranteed quality of service for
accepted traffic.

4. A network arrangement as claimed in claim 2, wherein said tunnels comprise multi-protocol label switched (MPLS) tunnels.
5. A network arrangement as claimed in claim 4, wherein each said tunnel comprises first and second tunnel portions coupled via a network node therebetween.
6. A network arrangement as claimed in claim 5, wherein said core network comprises an ATM network.
7. A network arrangement as claimed in claim 6, wherein at least one said gateway provides subscriber access to a voice network via the core network.
8. A network as claimed in claim 7, wherein one or more said terminals are coupled to the respective gateways via digital subscriber line access multiplexers (DSLAM).
9. A network as claimed in claim 8, wherein a plurality of said terminals are coupled to a said gateway via a campus local area network.
10. A label switched media gateway for controlling subscriber access to a connectionless core network in which user traffic is routed via tunnels established therein, the gateway providing an interface between a plurality of subscriber terminals and the network, and being arranged to route user traffic across the network via tunnels of guaranteed capacity reserved for that traffic.
11. A label switched media gateway for controlling subscriber access to a connectionless (IP) core network in which user traffic is routed via tunnels established therein, the gateway providing an interface between a plurality of subscriber terminals and the network, and being arranged to route user traffic across the network via tunnels of guaranteed capacity reserved for that traffic, the gateway comprising a plurality of proxies for translating IP

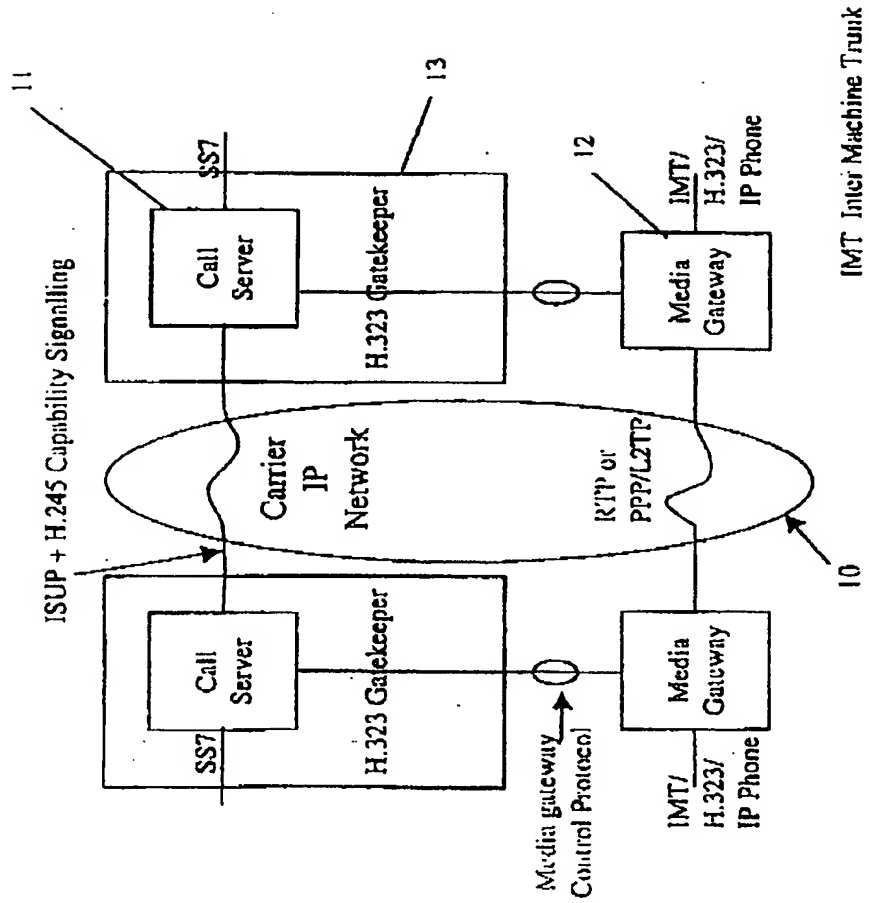
addresses between the network and encapsulated Layer 3 addresses, the latter constituting an address space which is allocated dynamically for session services to said subscribers.

- 5 12. A method delivering IP packet services to network subscribers, the method comprising establishing tunnels in the network, transporting said services in the tunnels whereby to provide security of that traffic from third party access, and accepting traffic into a said tunnel only where capacity is available so as to provide a guaranteed quality of service to traffic accepted into that tunnel.
- 10
13. A method of controlling subscriber access to a connectionless network so as to provided controlled delivery of services to that subscriber, the method comprising routing traffic to and from said subscribers via tunnels
- 15 established across the network, and controlling admission to a said tunnel by determining the currently available capacity of that tunnel so as to provide quality of service guarantees to traffic accepted into the tunnel.
14. A method of controlling subscriber access via edge nodes to a connectionless packet network so as to provided controlled delivery of IP packet services to the subscribers, the method comprising establishing a plurality of tunnels arranged in the network in a full mesh between said edge nodes, each said tunnel having a predetermined traffic handling capacity and each being exclusively reserved for carrying traffic between a respective pair of said edge nodes, determining in response to each subscriber request for service the available capacity of a said tunnel in which the subscriber traffic is to be routed, and accepting that subscriber request for service only if sufficient capacity is available in that tunnel so as to provide quality of service guarantees to accepted traffic.
- 20
- 25
- 30 15. A method as claimed in claim 14, an including appending two labels to each IP packet, the first label identifying the tunnel to be used, and the second identifying the destination gateway for that packet.

16. A method as claimed in claim 15, wherein, for virtual private intranet (VPI) access, a tunnel is established between the VPI and the gateway, and wherein routing is performed at Layer 3 using VPI addresses to access the established tunnel.

Smart & Biggar
Ottawa, Canada
Patent Agents

Figure 1 (Prior Art)



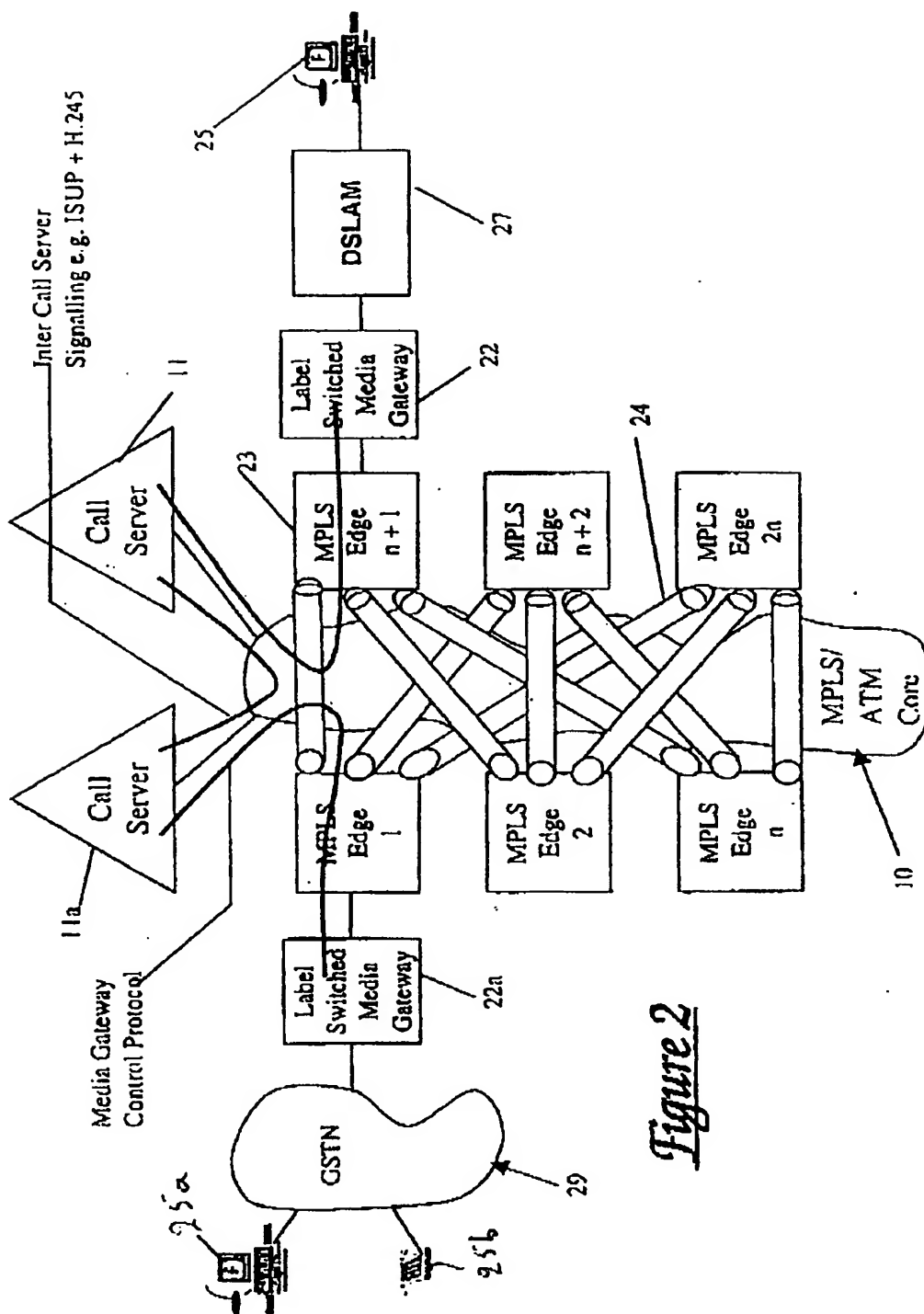


Figure 2

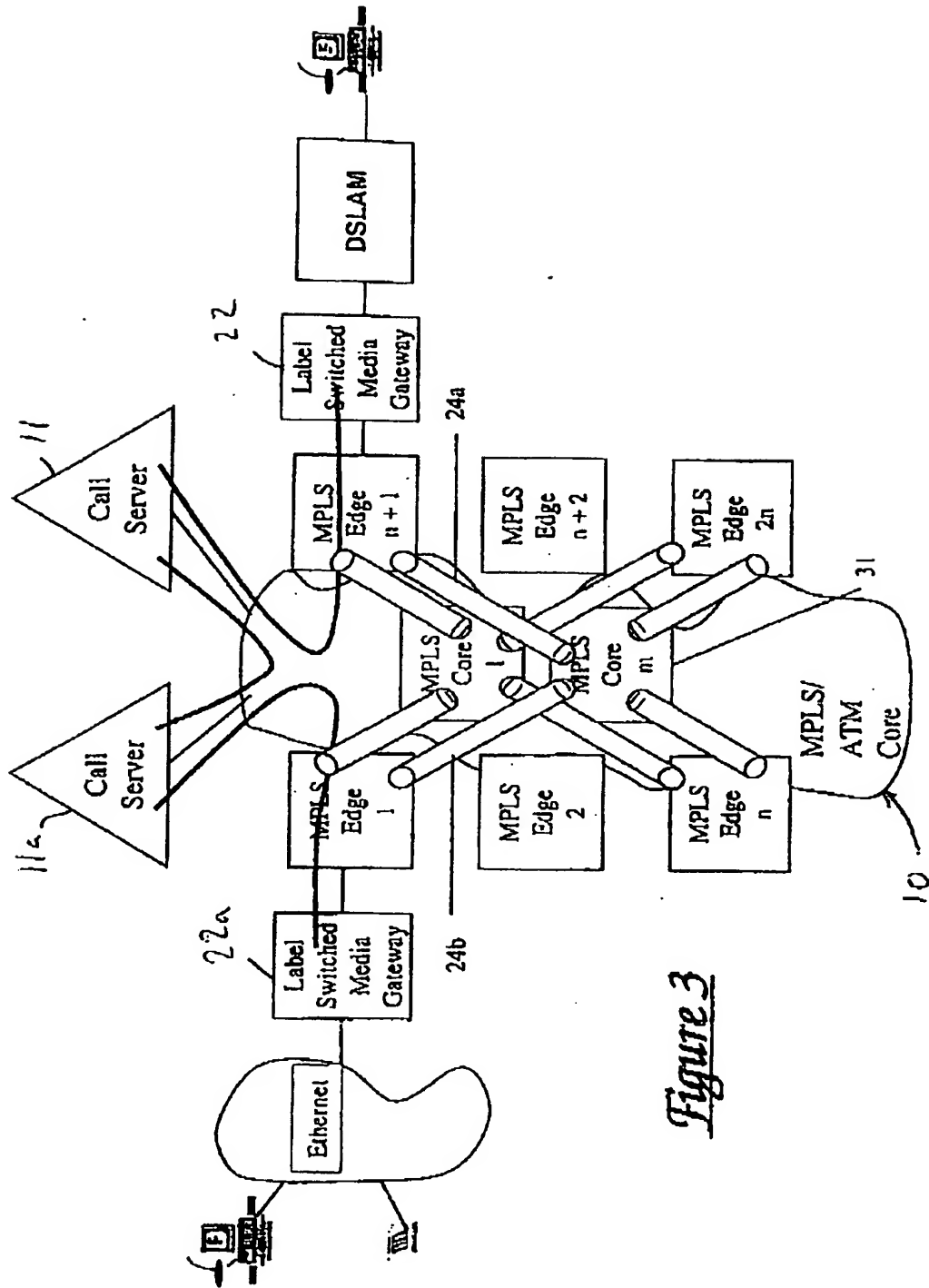


Figure 3

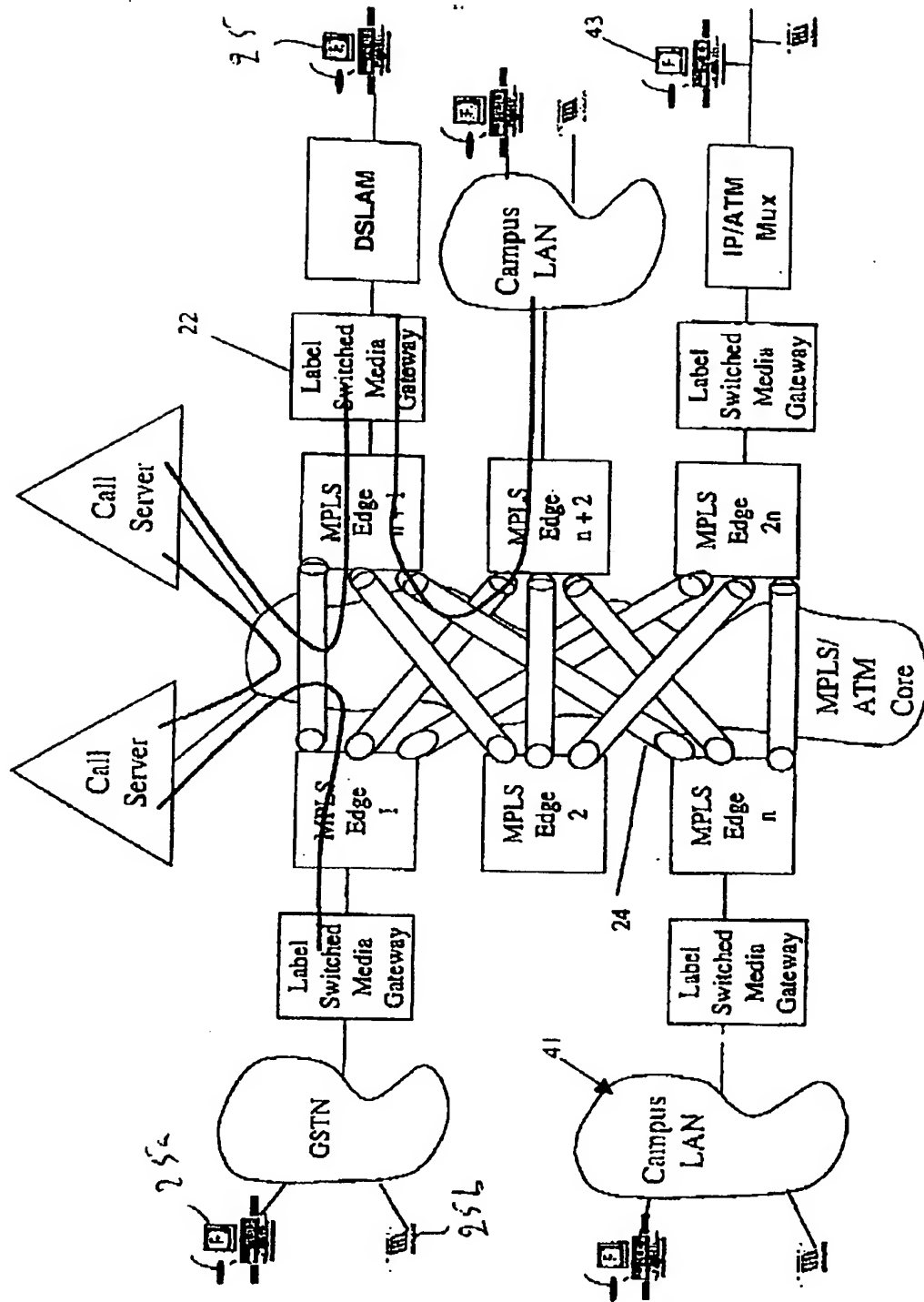


Figure 4

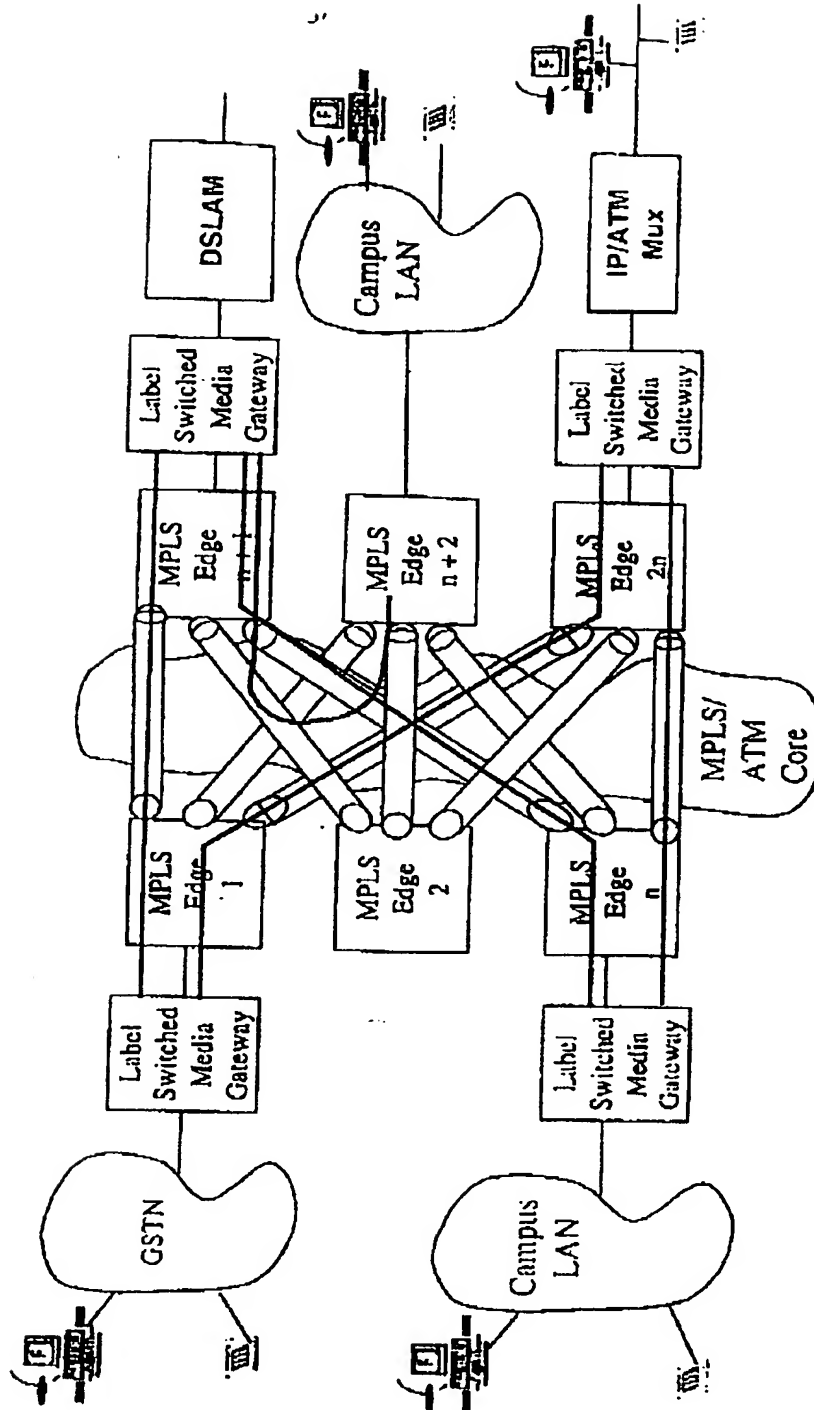


Figure 5

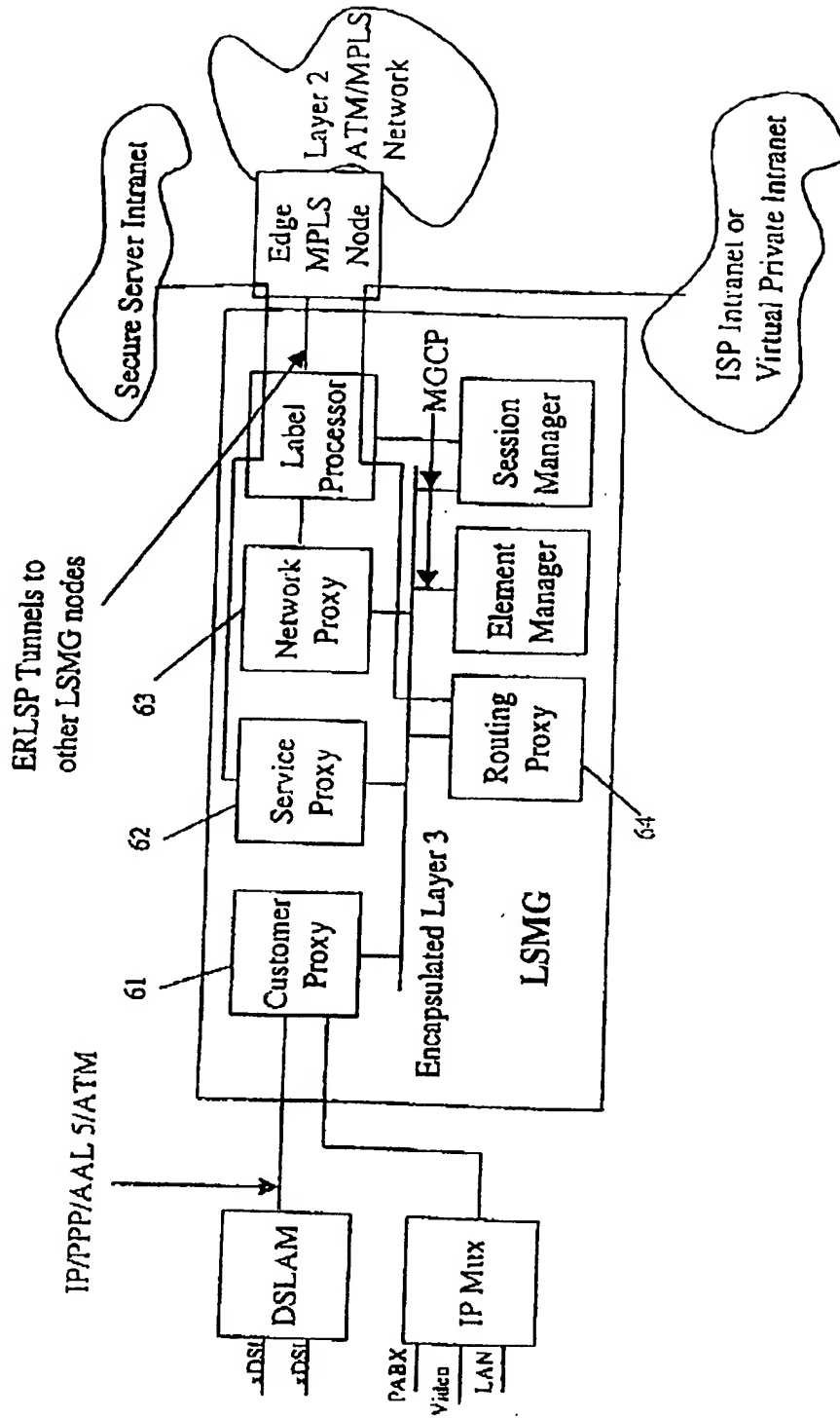
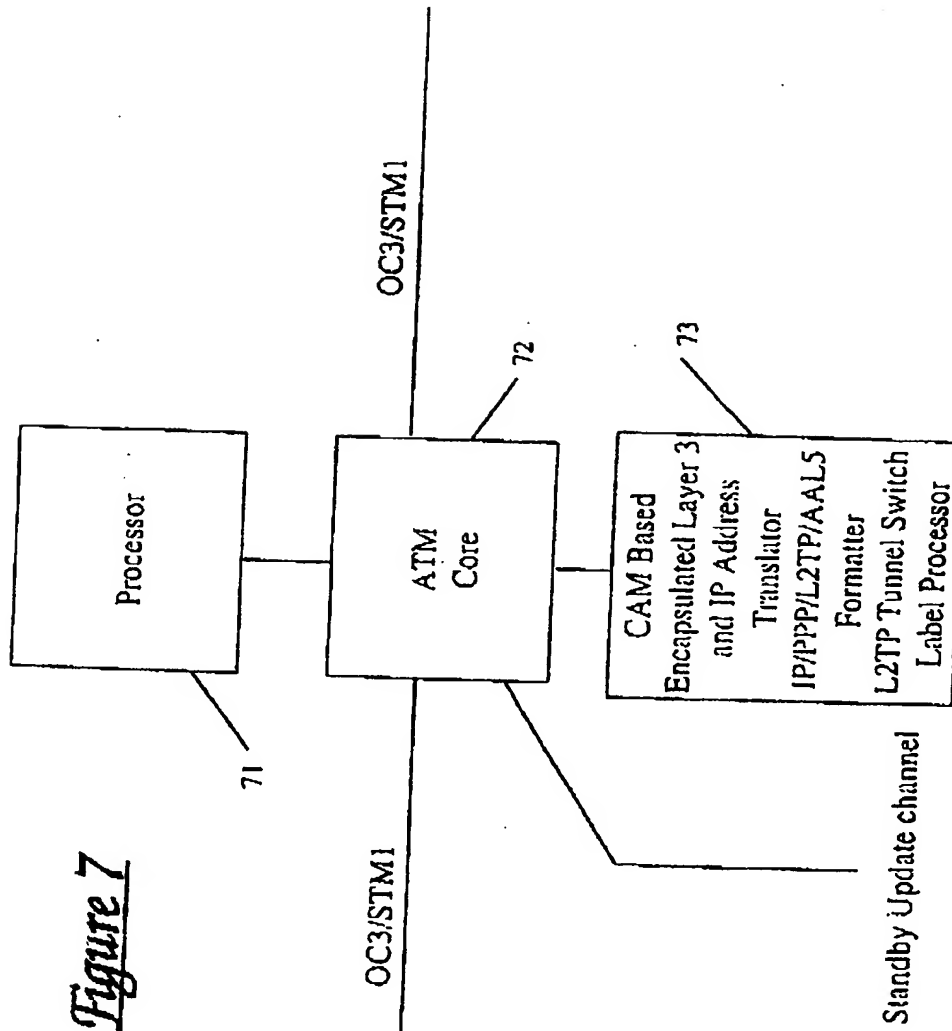


Figure 6

Traffic Module Functional Architecture

Figure 7



LSMG Server Functional Architecture

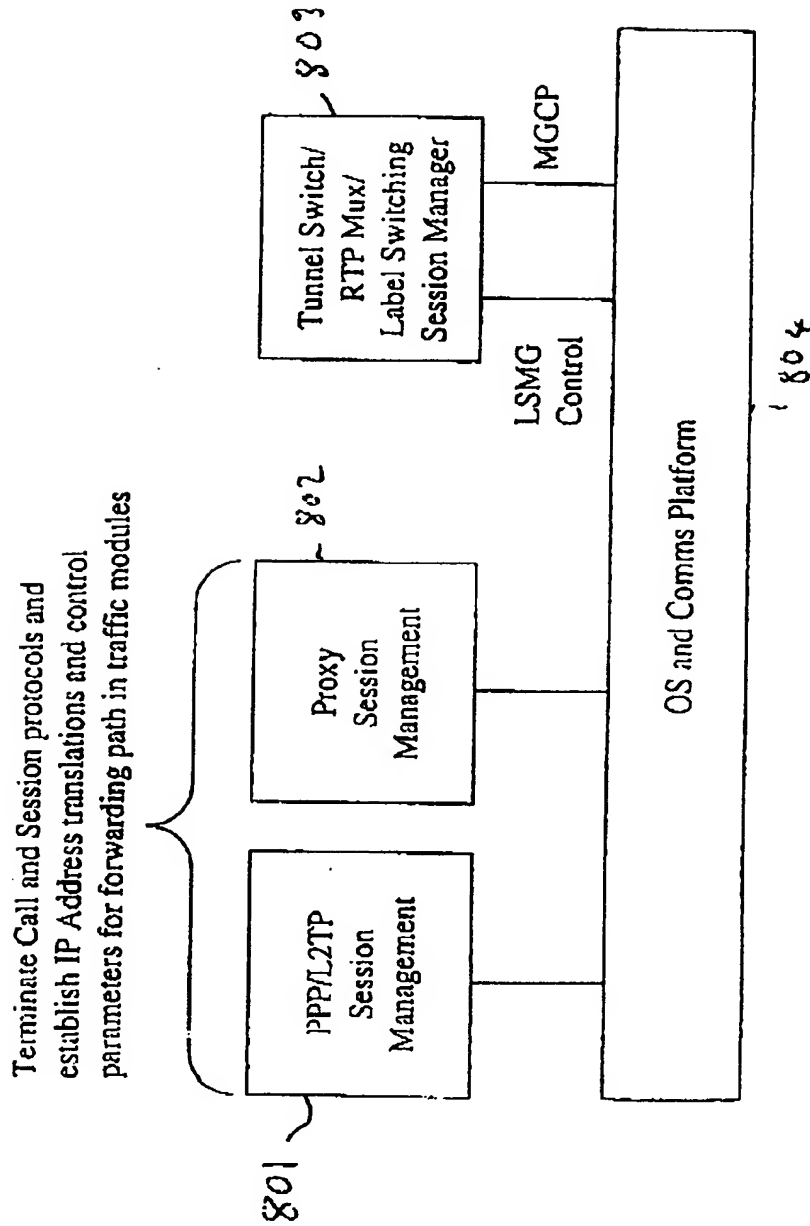


Figure 8

Call Flow for PSTN Call Setup

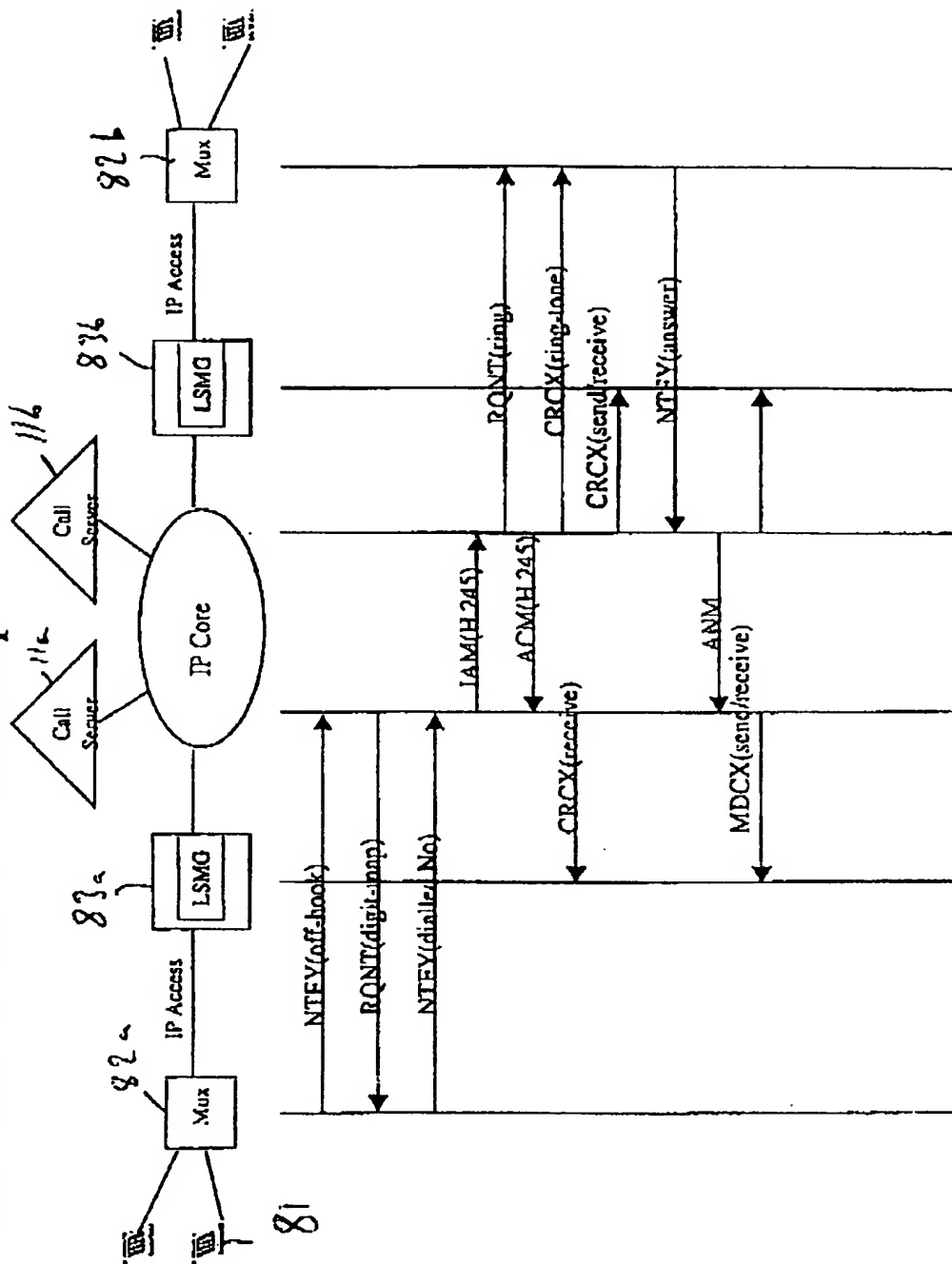


Figure 9